

Appln No. 09/690,243
Amdt date August 20, 2008
Reply to Office action of May 20, 2008

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A scalable on-line system for printing value bearing items (VBI) comprising:

a client system; and

a scalable server system communicating with the client system over a communication network comprising:

a database remote from the client system and including information about a plurality of users;

a plurality of transaction data records stored in the database to ensure authenticity of the plurality of users, ~~wherein each transaction data record includes information to restore the data record to its last known state, when the data record is next used~~; and

a plurality of stateless cryptographic devices remote from the client system and capable of authenticating and processing VBI printing requests from any of the plurality of users using a respective transaction data records stored in the database, wherein when a VBI printing request from a current user is received by the server system, an available cryptographic device from the plurality of cryptographic devices and the database cross-verify a copy of a last transaction data record stored in the database and stored in the available cryptographic device, before processing loads the current user's transaction data record and instantiates a user state in the transaction data record to process the VBI printing request requests from the current user, and wherein the server system sends a print authorization to the client system to print a VBI when the copy of the last transaction data record is cross-verified.

2. (Previously Presented) The scalable on-line system of claim 1, wherein each transaction data record is related to a user.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

3. (Previously Presented) The scalable on-line system of claim 2, wherein the transaction data record related to a user is loaded into a respective cryptographic module when the user requests to operate on a value bearing item.

4. (Previously Presented) The scalable on-line system of claim 3, wherein the transaction data record related to a user is updated and returned to the database.

5. - 7. (Cancelled)

8. (Previously Presented) The scalable on-line system of claim 1, further comprising computer executable code for load-balancing to distribute traffic among multiple cryptographic modules.

9. (Cancelled)

10. (Previously Presented) The scalable on-line system of claim 1, wherein the database is partitioned across a plurality of physical databases.

11. (Previously Presented) The scalable on-line system of claim 1, wherein each cryptographic device performs cryptographic function on a transaction related to the database.

12. (Previously Presented) The scalable on-line system of claim 1, further comprising computer executable code for password authentication to prevent unauthorized access to the database.

13. (Previously Presented) The scalable on-line system of claim 1, wherein the database stores a first set of one or more last database transactions and each cryptographic device

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction.

14. (Previously Presented) The scalable on-line system of claim 13, wherein each cryptographic device prevents further database transactions if the second set of one or more last transaction stored in the cryptographic module does not compare with the first set of one or more last transaction stored in the database.

15. (Previously Presented) The scalable on-line system of claim 1, wherein each cryptographic device includes a data validation subsystem for allowing the module to verify that data is up to date and an auto-recovery subsystem for automatically re-synchronize the module with the data.

16. (Previously Presented) The scalable on-line system of claim 1, wherein each cryptographic device includes a computer executable code for preventing unauthorized modification of data.

17. (Previously Presented) The scalable on-line system of claim 1, wherein each cryptographic device includes a computer executable code for ensuring proper operation of cryptographic security and VBI related meter functions.

18. (Previously Presented) The scalable on-line system of claim 1, wherein each cryptographic device includes a computer executable code for supporting multiple concurrent users.

19. (Previously Presented) The scalable on-line system of claim 1, wherein the database includes one or more indicium data elements, data for account maintenance, and data for revenue protection.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

20. (Previously Presented) The scalable on-line system of claim 1, wherein the database includes virtual meter information.

21. (Previously Presented) The scalable on-line system of claim 1, wherein the database includes descending register data.

22. (Previously Presented) The scalable on-line system of claim 1, wherein the value bearing item is a mail piece.

23. (Previously Presented) The scalable on-line system of claim 22, wherein postal indicium comprises a digital signature.

24. (Previously Presented) The scalable on-line system of claim 1, wherein a respective cryptographic device performs cryptographic function on validation information according to a user request for printing a VBI.

25. (Previously Presented) The scalable on-line system of claim 1, wherein a respective cryptographic device generates data sufficient to print a postal indicium in compliance with postal service regulation on a mail piece.

26. (Previously Presented) The scalable on-line system of claim 1, wherein the value bearing item is a ticket.

27. (Previously Presented) The scalable on-line system of claim 1, wherein a bar code is printed on the value bearing item.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

28. (Previously Presented) The scalable on-line system of claim 1, wherein the value bearing item is a coupon.

29. (Previously Presented) The scalable on-line system of claim 1, wherein the value bearing item is currency.

30. (Previously Presented) The scalable on-line system of claim 1, wherein the value bearing item is a voucher.

31. (Previously Presented) The scalable on-line system of claim 1, wherein the value bearing item is a traveler's check.

32. (Currently Amended) [[The]] A scalable on-line system of claim 1, for printing value bearing items (VBI) comprising:

a client system; and

a scalable server system communicating with the client system over a communication network comprising:

a database remote from the client system and including information about a plurality of users;

a plurality of transaction data records stored in the database to ensure authenticity of the plurality of users, wherein each transaction data record includes information to restore the data record to its last known state, when the data record is next used; and

a plurality of stateless cryptographic devices remote from the client system and capable of authenticating and processing VBI printing requests from any of the plurality of users using a respective transaction data records stored in the database, wherein when a VBI printing request from a current user is received by the server system, an available cryptographic device from the plurality of cryptographic devices loads the current user's transaction data record and

Appln No. 09/690,243
Amdt date August 20, 2008
Reply to Office action of May 20, 2008

instantiates a user state in the transaction data record to process the VBI printing requests from the current user,

wherein each transaction data record includes one or more of an ascending register value, a descending register value, a respective cryptographic module ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective module, expiration dates for keys, and a passphrase repetition list.

33. (Currently Amended) The scalable on-line system of claim [[1]] 32, wherein each transaction data record includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign module status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the module and the VBI are authentic.

34. (Currently Amended) The scalable on-line system of claim [[1]] 32, wherein each cryptographic module includes executable instructions to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

35. (Currently Amended) The scalable on-line system of claim [[1]] 32, wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address matching service subsystem, a SSL proxy server subsystem, and a web server subsystem.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

36. (Currently Amended) The scalable on-line system of claim [[1]] 32, wherein the database includes one or more of a postal database, a provider database, an e-commerce database, and a membership database.

37. (Currently Amended) The scalable on-line system of claim [[1]] 32, further comprising an address matching server for verifying a correct address specified by a user.

38. (Currently Amended) The scalable on-line system of claim [[1]] 32, further comprising a printer driver database for storing supported printer driver information.

39. (Currently Amended) A method for printing value-bearing items (VBI) via a communication network including a client system, and a server system, the method comprising the steps of:

~~accepting print requests from a plurality of users by the client system;~~

~~communicating the print requests to the server system receiving a printing request from a user using the client system over the communication network;~~

~~storing in a database remote from the client system a plurality of transaction data records, wherein each transaction data record includes information to restore the data record to its last known state, when the data record is next used;~~

~~ensuring authenticity of the plurality of users utilizing a respective transaction data record;~~

~~processing in a stateless manner each transaction data record in the server system;~~

~~authenticating by a cryptographic device any of the plurality of users in a stateless manner, utilizing one or more of the plurality of transaction data record stored in the database;~~

~~receiving a VBI printing request from a current user;~~

~~loading the current user's transaction data record in the cryptographic device; and~~

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

cross-verifying a copy of last transaction data record stored in the database and stored in an available cryptographic device, before processing instantiating a user state in the transaction data record to process the VBI printing request requests from the current user;

authenticating the user by the cryptographic device in a stateless manner utilizing a respective one-of the plurality of transaction data record stored in the database; and

printing a VBI requested by the user.

40. (Previously Presented) The method of claim 39, wherein each transaction data record is related to a user.

41. (Canceled)

42. (Currently Amended) The method of claim 39, further comprising the steps of updating and returning the transaction data record related to [[a]] the user to the database.

43. (Previously Presented) The method of claim 39, further comprising the step of adding at least one more cryptographic device, wherein each cryptographic device is capable of processing any of the plurality of transaction data records.

44. (Currently Amended) The method of claim 39, further comprising the step of authenticating [[a]] the user using any of [[the]] a plurality of cryptographic devices.

45. (Previously Presented) The method of claim 43, further comprising the step of load-balancing to route user requests to the at least one more cryptographic device.

46. (Previously Presented) The method of claim 43, further comprising the step of load-balancing to distribute traffic among the multiple cryptographic devices.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

47. (Currently Amended) The method of claim 39, further comprising the step of the authenticating any of ~~the one or more~~ a plurality of users using the cryptographic module.

48. (Original) The system of claim 1, further comprising the step of partitioning the database across a plurality of physical databases.

49. (Previously Presented) The method of claim 39, further comprising the step of encrypting database transactions using the cryptographic device.

50. (Original) The method of claim 39, further comprising the steps of verifying a user password before granting access to the database.

51. (Previously Presented) The method of claim 39, further comprising the steps of storing one or more last database transactions in the database; storing one or more last database transactions in the cryptographic device; and comparing the one or more last database transactions stored in the database with the one or more last database transactions stored in the cryptographic device to verify each database transaction.

52. (Previously Presented) The method of claim 39, further comprising the step of encrypting transactions related to the database using the cryptographic device.

53. (Previously Presented) The method of claim 39, further comprising the steps of storing one or more last database transactions in the database, storing one or more last database transactions in the cryptographic device for comparison with the one or more last database transactions stored in the database to verify each database transaction.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

54. (Previously Presented) The method of claim 53, further comprising the step of preventing further database transactions if the one or more last transaction stored in the cryptographic device does not compare with the one or more last transaction stored in the database.

55. (Previously Presented) The method of claim 39, further comprising the steps of preventing unauthorized modification of data using the cryptographic device.

56. (Original) The method of claim 39, further comprising the steps of verifying that the database is up to date.

57. (Previously Presented) The method of claim 39, further comprising the steps of automatically re-synchronizing the cryptographic device with the database.

58. (Previously Presented) The method of claim 39, further comprising the step of ensuring proper operation of cryptographic security and VBI related meter functions.

59. (Original) The method of claim 39, further comprising the steps of supporting multiple concurrent operators.

60. (Currently Amended) The method of claim 43, further comprising the steps of:
storing information about a number of last transactions in ~~a respective~~ an internal register of ~~each of the~~ cryptographic device ~~devices~~;
storing a table including the information about a last transaction in the database;
comparing the information saved in the ~~respective~~ cryptographic device with the respective information saved in the database; and
loading a new transaction data if the respective information stored in the cryptographic device compares with the respective information stored in the database.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

61. (Original) The method of claim 39, further comprising the step of storing data for creating one or more indicium, account maintenance, and revenue protection.

62. (Original) The method of claim 39, further comprising the step of printing a mail piece.

63. (Original) The method of claim 62, wherein the mail piece includes a digital signature.

64. (Original) The method of claim 62, wherein the mail piece includes a postage amount.

65. (Original) The method of claim 62, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

66. (Original) The method of claim 50, further comprising the step of printing a ticket.

67. (Original) The method of claim 39, further comprising the step of printing a bar code.

68. (Original) The method of claim 39, further comprising the step of printing a coupon.

69. (Original) The method of claim 39, further comprising the step of printing currency.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

70. (Original) The method of claim 39, further comprising the step of printing a voucher.

71. (Original) The method of claim 39, further comprising the step of printing a traveler's check.

72. (Currently Amended) [[The]] A method of claim 39, for printing value-bearing items (VBI) via a communication network including a client system, and a server system, the method comprising the steps of:

accepting print requests from a plurality of users by the client system;

communicating the print requests to the server system over the communication network;

storing in a database a plurality of transaction data records, wherein each transaction data record includes information to restore the data record to its last known state, when the data record is next used;

ensuring authenticity of the plurality of users utilizing a respective transaction data record;

processing in a stateless manner each transaction data record in the server system;

authenticating by a cryptographic device any of the plurality of users in a stateless manner, utilizing one or more of the plurality of transaction data record stored in the database;

receiving a VBI printing request from a current user;

loading the current user's transaction data record in the cryptographic device; and

instantiating a user state in the transaction data record to process the VBI printing requests from the current user,

wherein each of the transaction data records includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

73. (Currently Amended) The method of claim [[39]] 72, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms using the cryptographic device.

74. (Currently Amended) The method of claim [[39]] 72, further comprising the step keeping track of user accesses to a vendor website using a website database.

75. (Currently Amended) The method of claim [[39]] 72, further comprising the step of storing postal transaction data, financial transaction data, customer marketing information, commerce product information, meter license information, meter resets, meter history, and meter movement information in an offline database.

76. (Currently Amended) The method of claim [[39]] 72, further comprising the step of storing customer information, financial transactions, and information for marketing queries in a data warehouse database.

77. (Currently Amended) The method of claim [[39]] 72, further comprising the steps of authorizing and capturing funds from a customer's account and transferring the funds to a vendor's account using an e-commerce server.

78. (Currently Amended) The method of claim [[39]] 72, further comprising the step of verifying a correct address specified using a user using an address matching server.

Appln No. 09/690,243

Amdt date August 20, 2008

Reply to Office action of May 20, 2008

79. (Currently Amended) The method of claim [[39]] 72, further comprising the step of storing supported printer driver information in a printer driver database.